**Statement of R. James Caverly, Director, Infrastructure Coordination Division**
**US Department of Homeland Security**
**New York Field Hearing**
**September 26, 2005**

## Introduction

Good morning, Mr. Chairman and distinguished Members of this Committee. I appreciate this opportunity to speak with you regarding the current state of preparedness within the financial services sector, one year following the heightened threat level for the financial services sector.

We know al-Qaida targeted the U.S. financial sector critical infrastructure in the past and that this remains a potential target for the future. September 11th impacted the financial sector especially hard, with the simultaneous loss of critical financial infrastructure operational capacity and a precipitous loss of financial asset values. However, the financial sector remained resilient, and critical financial operations, including securities, trading resumed after only a few days of interruption.

Since September 11th other events, including the northeast power outage of August 2003, and the revelation of the financial casing reports in August 2004, continue to remind us that ensuring the financial sector is prepared for large-scale natural or man-made disruptions is essential

## National Infrastructure Protection Plan

The Department of Homeland Security is committed to working with our partners in State, local and tribal governments and the private sector to reduce the overall level of risk of terrorist attacks against our national critical infrastructure. We help the national critical sectors to reduce risk by examining the consequences of a potential attack; examining the vulnerability of critical sites and facilities to various modes of attack; and examining the potential threat — that is, the intent of terrorists to attack in a given place and their likelihood of success.

In working to reduce risk and protect critical infrastructure, DHS has three principal objectives:

- Provide resources and training to State and local governments and law enforcement for security enhancements
- Provide information to both public and private sectors on the threat environment, tactics and techniques of terrorists, common vulnerabilities and suggested protective measures
- Create information-sharing mechanisms that enable DHS stakeholders to share amongst themselves information and best practices detailing the unique aspects of their assets to better ensure that DHS has adequate situational awareness during a crisis or when faced with a specific threat.

These goals are being realized through the implementation of the National Infrastructure Protection Plan (NIPP). Directed by Homeland Security Presidential Directive 7 (HSPD-7), the NIPP is a unified national plan for the consolidation of critical infrastructure protection activities. The NIPP is a collaborative effort between the private sector, State, local, territorial and tribal entities and all relevant departments and agencies of the Federal government.

The cornerstone of the NIPP is a risk management framework that combines threat, vulnerability, and consequence information to produce a comprehensive, systematic, and informed assessment of national or sector risk that drives our risk reduction efforts in the critical infrastructure/key resources (CI/KR) sectors. This framework applies to the general threat environment as well as specific threats or incident situations.

**NIPP Risk Management Framework**

The National Infrastructure Protection Plan incorporates the following objectives:

**Set Security Goals.** Achieving a secure, protected, and resilient infrastructure requires a common set of national and sector-specific security goals that address those aspects of risk that can be affected and collectively represent an acceptable security posture. Nationally, the overall security goal of risk reduction efforts is an enhanced state of CI/KR security achieved through implementation of focused risk reduction and protective strategies across the critical sectors.

**Identify Assets.** Once security goals are set, the next step in the framework is to develop and maintain an inventory of the Nation's critical assets. To identify these assets, DHS uses a screening process that helps us to identify those assets that present the greatest risk. However, before screening the assets, asset information is collected and catalogued in the National Asset Database, which is the central Federal repository for national infrastructure-related information. After an asset is identified and basic information on it is collected, DHS employs an initial screening methodology to determine whether or not it is of national consequence.

**Assess Risk.** If an asset is determined to of national consequence, it is then subjected to a risk analysis. As mentioned before, risk is determined by combining assessments of:

- Consequence — estimates of the damage that a successful attack would cause
- Threat — estimates of the likelihood that a particular target or type of target will be selected for attack.
- Vulnerability analysis determines which elements of infrastructure are most susceptible to attack and how attacks against these elements would be most likely be carried out.

One of the Department's principal risk-assessment tools is RAMCAP (Risk Assessment Methodology for Critical Asset Protection). RAMCAP is currently being developed by DHS in collaboration with other federal agencies and the private sector as a sector-

specific consequence, vulnerability, and risk methodology. RAMCAP will allow DHS to assess national critical infrastructures according to these factors and allows us to compare assets from across sectors and better prioritize our protective efforts.

**Prioritize.** It is impossible to protect all CI/KR equally across the entire United States. Because the potential consequences of an attack, threats, and vulnerabilities differ for individual assets and sectors, analysis is necessary to understand and prioritize risk across the infrastructure or various segments. Such analysis identifies high-risk assets that become the focus of longer-term resource decisions, strategic protective programs, and planning for response and other contingency situations. This, in turn, supports the informed allocation of resources and is the primary goal of the risk management framework.

**Implement Protective Programs.** The highly distributed nature of infrastructure demands distributed ownership and execution of protection programs, but it also requires centralized leadership to drive consistent implementation and ensure the greatest cost-benefit. DHS leads the Federal critical infrastructure protection effort, and works in collaboration with State and local government, the private sector, and our international partners to reduce our vulnerability to, among other things, bombing attacks, and to enhance our capability to respond if such an attack takes place.

**Financial Sector Coordinating Councils**

Private sector-led Sector Coordinating Councils (SCCs) and their counterpart, Government Coordinating Councils (GCCs), provide an important mechanism for effective public-private partnerships, information sharing, and coordination for the entire range of critical infrastructure protection, recovery, and response activities, both within and across sectors. Under the NIPP framework, DHS is encouraging the creation of SCCs for each of the 17 critical infrastructure/key resource (CI/KR) sectors. These councils are self-organized and self-governed and composed of sector owners and operators and their representative organizations. GCCs have been formed to achieve inter-agency coordination and information sharing on critical infrastructure protection activities. Like the SCCs, the GCCs coordinate strategies, activities, policy, and communication across organizations within each sector. The SCCs and GCCs serve as points of entry, coordination, and collaboration between government and industry in the sector.

The financial service sector has well-established coordinating council structures already in place. The sector is coordinated by the Financial Services Sector Coordinating Council (FSSCC), representing private sector companies, and the Financial and Banking Infrastructure Information Council (FBIIC), representing government regulators. The mission of the two groups is to improve the reliability and security of financial information infrastructure and to improve critical infrastructure protection and homeland security.

The FSSCC, a network of financial trade associations and private firms representing thousands of financial services organizations, works closely with the U.S. Department of

the Treasury, financial regulators, and the FBIIC to coordinate the private sector's work to identify and reduce vulnerabilities in the financial services sector infrastructure to organized attacks, criminal or illegal activities, or other disruptive events that may occur, to ensure the resilience of the nation's financial services sector infrastructure, and to promote public trust and confidence in the financial services sector's ability to withstand and recover from events that may occur.

**Financial Sector Heightened Alert Level**

The financial sector's vigilance in strengthening its resilience and crisis response procedures was clearly illustrated in its rapid response to last year's August elevation of the Homeland Security Threat Advisory level for the financial services sector in New York, northern New Jersey, and Washington, DC.

On August 1, 2004, the day the threat level was elevated, DHS held numerous urgent conference calls with sector entities, including the FSSCC, FBIIC, and the Financial Sector Information Sharing and Analysis Center (FS/ISAC), an organization that facilities communication and collaboration among financial sector firms on critical security threats facing the sector, providing the sector with advance notification of the pending threat level change, allowing the sector to rapidly strengthen security in and around specific buildings and locations as well as throughout the financial services sector.

Subsequent to providing immediate alerts to the financial sector regarding the threat, DHS's Infrastructure Protection (IP) Division continued to work with the industry to ensure that all targeted financial institutions were individually briefed. IP coordinated with Federal, State, and local law enforcement (LLE) entities to ensure that the appropriate information was exchanged between the government and the private sector. IP also polled the various financial institutions to determine what additional protective measures were implemented as a result of the heightened alert. This included the deployment of IP personnel to provide technical assistance, identify security gaps and provide federal resources to LLE and facility owners and operators.

Teams of IP personnel, in collaboration with local law enforcement officials and asset owners and operators, have conducted Site Assistance Visits (SAVs) to facilitate vulnerability identification and to discuss protective measure options. A total of 15 visits have been conducted thus far of facilities in the banking finance sector.

In addition to SAVs, IP personnel have been working with individual facilities and LLE entities to implement buffer zones around select banking and finance assets. The Buffer Zone Protection Program (BZPP) is a community-based effort focused on rapidly reducing vulnerabilities "outside the fence" of select CI/KR. To support these efforts, IP provides assistance to LLE officials to develop and implement buffer zone plans. To date, seven buffer zone plans for the banking and finance sector have been submitted to IP by State Homeland Security Advisors and are eligible for $350,000 in BZPP grants.

Based on data gathered from SAVs and BZPPs, DHS has developed five Characteristics and Common Vulnerabilities (CV) and Potential Indicators of Terrorist Activity (PI) reports for the banking and finance sector. CV/PI reports identify the common characteristics and vulnerabilities of sector assets and provide information on how to detect terrorist activity near critical sites. These reports have been distributed to all State Homeland Security Offices, with guidance to share these reports with the owners/operators of critical infrastructure and the law enforcement community within each State.

Information gathered from SAVs and BZPPs, and updates from the threat data, was given to the Principal Federal Official (PFO) in New York City. IP personnel were assigned to the PFO staff to provide expert, subject-based knowledge and act as a conduit to resources held by the rest of the department. IP supported the New York PFO in the days leading up to and during the Republican National Convention with updated information, technical expertise, and material assistance when appropriate.

Protective Security Advisors (PSAs) are also stationed in New York City, Chicago, Washington, DC, San Francisco and other major cities with a large financial sector presence to represent DHS in local communities throughout the United States. PSAs serve as a liaison between DHS, the private sector, and Federal, State, local, and tribal entities and work to assess, prioritize, and secure critical infrastructure within a community.

After the August 2004 elevation of the threat level for the banking and finance sector, additional steps were taken to strengthen emergency preparedness and response by improving communications systems and protocols between and among financial regulators and critical financial institutions; assessing and reviewing business continuity plans; and participating in numerous drills and exercises to test backup systems and prepare financial professionals. These additional protective measures were permanent and sustainable enhancements that continue to be followed today, further reducing the possibility of attacks.

**Improving Telecommunications Resilience**

The financial services sector is reliant not only on its own resources and infrastructures to support its businesses, but also on several other key sectors, foremost the telecommunications and electricity sectors. This dependency on the telecommunications sector was the focus of attention in 2004, with several groups taking action to explore this dependency in much greater detail and to develop recommendations on how sector members can address and minimize it.

IP supported the development of the National Security Telecommunications Advisory Committee's (NSTAC) April 2004 "Financial Services Task Force Report." This report provided a thorough review interdependency issues and offered information and recommendations to the sector in addressing the diversity, redundancy, and recoverability

of its critical systems. DHS's Infrastructure Protection Division was represented on this work.

**Protection and Enhancement of Telecommunication Capabilities**

Over the past year, DHS has worked extensively to enhance telecommunications resiliency for the financial sector.

The National Communications System (NCS) conducted several activities which address the national goals, objectives, milestones, and key initiatives with regard to critical infrastructure protection as outlined in the NIPP. The NCS has worked with the Department of Treasury, the Federal Reserve Board (FRB), and other financial services institutions in the following efforts:

- **Development of the Route Diversity Methodology (RDM).** Route diversity (RD) is communications routing between two points over physically separate paths. The NCS developed RD recommendations for the FRB to enhance telecommunications resiliency for its Washington, DC location. Using the RDM, the FRB assessed the physical diversity and resiliency of its voice and data telecommunication systems. The RDM was also used to identify vulnerable assets and to develop mitigation strategies.

- **Enhanced Analysis Capabilities.** The NCS continues to enhance and expand its existing analysis capabilities, tools, and data sets to better assess the impact of various scenarios on the banking and finance community. The Operational Analysis Branch routinely provides the Information Analysis and Infrastructure Protection Directorate regional information identifying financial institutions' dependencies on the telecommunications infrastructure. Furthermore, the NCS recently conducted the Internet Disruption and Impact Analysis study to determine the reliance of various sectors, including the financial services sector, on the Internet in New York and Washington, DC, yielding results that identified critical service providers and assets.

- **Awareness of the Alliance for Telecommunications Industry Solutions' National Diversity Assurance Initiative.** On June 3, 2004 the Alliance for Telecommunications Industry Solutions' (ATIS) Chief Information Officers Council and the Federal Reserve Board agreed to form a partnership, known as the National Diversity Assurance Initiative (NDAI), to conduct an in-depth assessment of diversity assurance to the financial services sector including researching the feasibility of validating the existence of diversity on critical national security and emergency preparedness (NS/EP) circuits and identifying methods to assure that diversity is maintained on those circuits over time. Since the establishment of the NDAI and per its NS/EP mission, the NCS has maintained an awareness of the group's activities to remain informed on issues pertaining to national security telecommunications.

**Homeland Security Information Network**

The purpose of the Homeland Security Information Network (HSIN) is to provide a user friendly, secure and effective medium for the timely sharing of information between governmental entities at all levels (Federal, State, tribal, local and territorial), Private Sector organizations, and International partners. The HSIN system will also provide a secure and effective vehicle for collaboration among those entities, enhancing their combined effectiveness in preventing and responding to terrorist attacks and preparing for and responding to natural and man-made disasters.

HSIN-Critical Sector (CS) provides a common communications platform to encourage sector-wide planning, coordination, and information sharing. This platform will deliver an improved situational and operational awareness of the nation's critical infrastructures and key resource (CI/KR) sectors to both the public and private sector. HSIN-CS allows operators within a critical sector to share information in a secure manner with each other and with government and allows government to share its analytic capabilities and reports directly with a sector. HSIN-CS will be the primary tool for DHS to share security threat information with specific sectors.

HSIN-CS is being been deployed through the engagement by DHS with various Sector Specific Agencies (SSAs) and Government and Sector Coordinating Councils (GCCs/SCCs). Private and Public Sector owners and operations of CI/KR are encouraged to voluntarily participate on HSIN. Eleven HSIN-CS pilots have been successfully launched. Several more are in progress.

DHS will continue to explore the use of HSIN as a no-cost approach to reach 100 percent of the CI/KR sector members.

**Conclusion**

Since the threat level was raised on August 1, 2004, DHS in conjunction with Federal, State and local leaders as well as the private sector have worked hard to strengthen security in and around specific buildings and locations, and throughout the financial services sector. Today there are permanent protective measures in place that did not exist before August 1. These new measures include increased security at the affected buildings, enhanced screening measures, increased perimeter protection and the development of security buffer zone protection plans.

The financial services sector as also taken additional steps to strengthen emergency preparedness and response by improving communications systems and protocols between and among financial regulators and critical financial institutions; assessing and reviewing business continuity plans; and participating in numerous drills and exercises to test backup systems and prepare financial professionals.

DHS remains dedicated to working with infrastructure stakeholders across the country to increase the security and protection of our Nation's critical infrastructure sectors. Thank you. I would be pleased to answer any questions you may have at this time.